RUSS, AUGUST & KABAT
Reza Mirzaie (CA SBN 246953)
rmirzaie@raklaw.com
Marc A. Fenster (CA SBN 181067)
Email: mfenster@raklaw.com
Brian D. Ledahl (CA SBN 186579)
Email: bledahl@raklaw.com
Benjamin T. Wang (CA SBN 228712)
Email: bwang@raklaw.com
Paul A. Kroeger (CA SBN 229074)
Email: pkroeger@raklaw.com
Kent N. Shum (CA SBN 259189)
kshum@raklaw.com
Jonathan Ma (CA SBN 312773)
jma@raklaw.com
12424 Wilshire Boulevard, 12th Floor
Los Angeles, California 90025
Telephone: (310) 826-7474
Facsimile: (310) 826-6991

Attorneys for Plaintiff
PROVEN NETWORKS, LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PROVEN NETWORKS, LLC

Plaintiff,

v.

F5 NETWORKS, INC.,

Defendant.

Case No. 5:20-cv-5571

COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq.*, in which Plaintiff Proven Networks, LLC ("Plaintiff" or "Proven Networks") makes the following allegations against Defendant F5 Networks, Inc. ("Defendant"):

PARTIES

1. Plaintiff Proven Networks, LLC is a company organized under the laws of the State of California. Proven Networks is the sole owner by assignment of all right, title, and interest in each Asserted Patent.

2. On information and belief, Defendant F5 Networks, Inc. is a corporation organized under the laws of the State of Washington, with its principal place of business at 801 5th Avenue, Seattle Washington 98104.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant in this action because Defendant has committed acts within this District giving rise to this action, and has established minimum contacts with this forum such that the exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice. Defendant, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, making, using, importing, offering to sell, and selling products that infringe the Asserted Patents.

5. Venue is proper in this District under 28 U.S.C. § 1400(b). Defendant is registered to do business in California, and upon information and belief, Defendant has transacted business in this District and has committed acts of direct and indirect infringement in this District by, among other things, importing, offering to sell, and selling products that infringe the asserted patents.

Defendant has a regular and established place of business in the District, including corporate offices at 3545 North 1st Street, San Jose, California 95134.[1]

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 7,450,507

6. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

7. Plaintiff owns by assignment all rights, title, and interest in U.S. Patent No. 7,450,507 ("'507 Patent") titled "Hierarchal Rate-Limiting at a Network Node that Utilizes an Infinity Rate-Limit Check." A true and correct copy of the '507 Patent is attached hereto as Exhibit 1.

8. The '507 Patent was duly and legally issued by the United States Patent and Trademark Office on November 11, 2008.

9. Computer networks are not limitless mediums. They have finite capacities and limits on the maximum rate of data that can be transferred across the network, what is often broadly referred to as bandwidth. And at each of the various layers in a network, of which there may be many, there are further bandwidth limits (*e.g.*, the Port, IP subnet, Protocol, and Socket layers). Bandwidth limitations in a network are a product of the underlying network architecture, and allocations that may be made at each layer. Due to the inherent limits on the amount of available bandwidth in a given network, computer engineers have developed countless strategies to optimize network traffic, whether through hardware, software or a combination of the two.

10. Amongst the universe of ways to optimize a computer network, the '507 Patent targets the management of traffic streams from network nodes through rate-limiting. Rate-limiting is a process of limiting the amount of traffic that is allowed from a network node. Ex. 1 at 1:19-

[1] *See, e.g.*, https://www.f5.com/company/contact/regional-offices.

21. Rate limiting may be applied in a hierarchical scheme, meaning that rate-limits are applied to different layers of a data flow or different classifications or subclassifications of the data in a data stream. *Id.* In the '507 Patent, one example is that traffic at the Socket level must not exceed 20 Megabits per second, traffic at the Protocol level must not exceed 100 Megabits per second, "traffic at the IP subnet (IP1) level ... must not exceed 500 Megabits per second and the overall traffic at the port level ... must not exceed 1 Gigabit per second." *Id.* at Fig. 2, 5:13-16.

11. Through the use of rate-limits, network providers can manage the amount of traffic in the computer network to optimize network performance. If a node exceeds a given rate-limit, or traffic at a certain classification becomes oversubscribed, network systems may then de-prioritize the data packet, hold it, or drop it to relieve the amount of traffic. Ex. 1 at 5:55-63, 10:7-11. In a hierarchical rate-limiting scheme, the traffic stream must pass each rate-limit associated with its classifications, in which case the traffic is given an "overall" pass to proceed.

12. Hierarchical rate-limiting schemes themselves, however, are prone to inefficiencies. A particular data flow might fail one or more of its rate limits when there might still be network bandwidth allocated to different layers that are available. Network engineers therefore implemented borrowing schemes to allow classifications at various layers to "borrow available bandwidth from the allocated rate limit of their parent classification." Ex. 1 at 1:50-55. At the time of the invention there were software schemes to enable rate-limiting borrowing schemes, and more problematic hardware implementations of the same. *Id.* at 1:49-2:3. Hardware approaches were considered more difficult and caused "additional latency for the traffic and/or additional complexity in hardware to [reallocate bandwidth] at the desired speeds." *Id.* at 1:64-2:3.

13. The inventors of the '507 Patent, computer network experts at Alcatel-Lucent, invented a new hierarchical rate-limiting scheme using what they called an "infinity rate-limit check." "The infinity rate-limit rule extends the life of [a] packet so that the ultimate determination of whether or not to grant an overall pass to the packet is made in a higher classification level than

the traffic classification level in which the packet did not receive a pass. That is, the infinity rate-limit rule grants an automatic pass to the packet at the child classification level regardless of the outcome of the rate-limit check of the child classification level .... By granting an automatic pass to the packet at the child classification level, **the infinity rate-limit rule enables available bandwidth to be borrowed from the parent classification level so that the packet receives an overall pass, regardless of whether the packet passed the rate-limiting rule of the child classification level**." *Id.* at 5:27-39 (emphasis added). And the inventors explained the improvements to the computer network in that "[u]tilizing infinity rate-limit rules to allow borrowing of bandwidth from an infinity rate-limit check enables more efficient combinatorial rate limiting (*i.e.*, for packets belonging to more than one classification of traffic) and enables hierarchal rate-limiting to be implemented economically, efficiently, and with minimal packet latency in hardware." *Id.* at 3:20-26.The "infinity rate-limit check" ensures that so long as a packet passes the rate-limit associated with its highest associated classification, and there is available bandwidth, the packet will be able to borrow that bandwidth so that it may continue through the network. Contemporaneous hierarchical rate-limiting schemes lacked this "infinity rate-limit check" and lacked the ability to provide an "overall" pass even if a packet failed a lower level rate-limit check. *See* Ex. 2 at 2 (Patent Office's Notice of Allowability).

14. The claims of the '507 Patent are directed to an infinity rate-limit check in a hierarchical rate-limiting scheme to enable borrowing of bandwidth available at higher layers in the network. The infinity rate-limit check enables bandwidth borrowing from higher packet classification levels even if the packet fails a lower level rate-limit check. The infinity rate-limit check was a new, specific computer technique that improved computer networks by ensuring a more efficient use of available bandwidth. By using an infinity rate-limit check, network administrators can override a failed rate-limit check at a given classification and still ensure the packet receives an overall pass if the rate-limit check for the layer above is passed.

15. The infinity rate-limit check is the claimed advance of the '507 patent, what distinguished it from prior art rate-limit schemes, and what led to the allowance of the '507 patent claims by the Patent Office. Ex. 2 at 2.

16. Moreover, use of the '507 Patent's infinity rate-limit check resulted in a new kind of hierarchical rate-limit scheme that enabled computer networks to reallocate, or borrow, available bandwidth in a manner that was not done before. The Patent Office expressly recognized this in its Notice of Allowability, stating that "[t]he prior art of record fails to teach or make obvious the steps of or means for 'granting an overall pass of said rate-limit hierarchy if said packet passes said first rate-limit check, even if said packets fails second rate-limit check', when the granting is considered within the specific combination of steps recited in the method of claim 1." Ex. 2 at 2. And consistent with that finding, the inventors explained during the prosecution that other hierarchical rate-limit scheme at the time did not grant packets an overall pass "even if said packet fails said second rate-limit check." Ex. 3 at 7; *see also* Ex. 4 at 7.

17. The "infinity rate-limit check" of the '507 patent was not a well-understood, routine or conventional technique for managing traffic in a computer network. The patent, for instance, confirms that the "infinity rate-limit check" resulted in a new and improved computer network: "[u]tilizing infinity rate-limit rules to allow borrowing of bandwidth from an infinity rate-limit check **enables more efficient combinatorial rate limiting** (*i.e.*, for packets belonging to more than one classification of traffic) and **enables hierarchal rate-limiting to be implemented economically, efficiently, and with minimal packet latency** in hardware." Ex. 1 at 3:20-26 (emphasis added). The inventors repeatedly explained during prosecution that it was the novel use of the infinity rate-limit check that enabled functions that did not exist in hierarchical rate-limit schemes of the time. Ex. 2 at 7 (explaining that prior art did not grant packets an overall pass "even if said packet fails said second rate-limit check"); Ex. 3 at 7 (same). The Patent Office agreed, stating in its Notice of Allowability that "[t]he prior art of record fails to teach or make

obvious the steps of or means for 'granting an overall pass of said rate-limit hierarchy if said packet passes said first rate-limit check, even if said packets fails second rate-limit check', when the granting is considered within the specific combination of steps recited in the method of claim 1." Ex. 2 at 2. Accordingly, the '507 patent describes and claims an inventive concept.

18. On information and belief, Defendant makes, uses, offers for sale, sells, and/or imports certain products ("Accused Products"), such as the F5 Network BIG-IP Policy Enforcement Manager (PEM), that directly infringe, literally and/or under the doctrine of equivalents, claims 1–20 of the '507 Patent.

19. Defendant also knowingly and intentionally induces infringement of claims 1–20 of the '507 Patent in violation of 35 U.S.C. § 271(b). At least through the filing and service of the Complaint in Case No. 3:20-cv-02521, Defendant has knowledge of the '507 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '507 Patent, Defendant continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website) to use the Accused Products in ways that directly infringe the '507 Patent. Defendant does so knowing and intending that its customers and end users will commit these infringing acts. Defendant also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '507 Patent, thereby specifically intending for and inducing its customers to infringe the '507 Patent through the customers' normal and customary use of the Accused Products.

20. The Accused Products satisfy all claim limitations of claims 1–20 of the '507 Patent. A claim chart comparing independent claim 1 of the '507 Patent to the representative Accused Product, the F5 Network BIG-IP Policy Enforcement Manager (PEM), is attached as Exhibit 5.

21. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Defendant has injured Plaintiff and is liable for infringement of the '507 Patent pursuant to 35 U.S.C. § 271.

22. As a result of Defendant's infringement of the '507 Patent, Plaintiff is entitled to monetary damages in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendant, together with interest and costs as fixed by the Court.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 7,877,786

23. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

24. Plaintiff owns by assignment all rights, title, and interest in U.S. Patent No. 7,877,786, titled "Method, Apparatus and Network Architecture for Enforcing Security Policies Using an Isolated Subnet." The '786 Patent was duly and legally issued by the United States Patent and Trademark Office on January 25, 2011. A true and correct copy of the '786 Patent is attached as Exhibit 6.

25. The '786 Patent explains that it "relates to the field of data networks and, more specifically, to methods of protecting network systems from viruses and other malicious applications by enforcing security policies using an isolated sub-network." Ex. 6 at 1:7-11. Those methods, as claimed, even more specifically, expressly require the combined use of security policies of an "active format," examining conformance with security policies by examining a token, and restricting non-conforming clients to a subset of virtual local area networks in a specific way – using a specific type of protocol – an "extensible authentication protocol" ("EAP") to authenticate the client as a valid user of only a subset of available VLANs. In this way, network

resources are "protected," and safely isolated clients, as required by other claims, may then obtain current security policies in isolation to gain access to the network.

26. As explained in the '786 Patent, as the Internet has grown, so too has the "transmission of computer viruses, worms and other malicious applications." Ex. 5 at 1:19-21. "[B]efore the advent of the Internet and local intranets, users rarely read or copied data onto their computers from unknown external sources." *Id.* at 1:22-24. "[U]sers today, however, routinely receive data from unknown computers ... or via ... the world-wide-web using, for example, a web browser. As such, any company or service provider providing network access is concerned with security." *Id.* at 1:24-29.

27. As the '786 patent explains, virus protection systems at the time the patent was filed "focus[ed] on identifying and removing viruses from a system. The virus protection programs protect the computer by scanning e-mail and other files for known sections of a virus or worm. Whenever a file is identified as containing a known virus or worm, the user is alerted and the file can be removed or the virus within the file may be removed. Whenever a new virus is identified, new code is written to search for the identifiable features of the new virus." *Id.* at 1:37-45.

28. The inventors of the '786 patent, however, saw those systems as deficient. Those systems could only search for already known viruses and worms. "[T]he virus protection software will not know what the identifiable features of the new virus are and will thus not find it when it scans the files." *Id.* at 1:48-50. In addition, those systems were client-dependent. Virus protection software needed to be pre-installed on the client to scan for viruses, and as a result, security enforcement was dependent on end-users and inflexible. *Id.* at 4:66-5:5.

29. The claims of the '786 patent addressed those particular problems in computer networks and network security systems with a very specific, server-centric, model. It ensures conformance with security policies, focused on active format security policies, which can automatically run and update the client device, and forces non-conforming clients to isolated sub-

networks. These sub-networks are logically separated, virtual local area networks used to ensure the protection of "the rest of the IP network ... and in particular ... network resources of the IP network ... , such as file servers, other clients, web servers , etc." *Id.* at 4:41-47. Further, the system checks conformance with security policies through the use of a token, and then restricts non-conforming clients through an extensible authentication protocol (EAP). The use of an EAP, which is server initiated, complimented the server-centric and sub-network architecture of the invention, and avoided the client-dependent virus protection programs of the prior art. And so isolated in the sub-network, clients could safely "download[] and run[] the client software to update the security policies of the client in order to obtain access to the" rest of the network. *Id.* at 6:10-14.

30. The '786 patent protects network systems, and explains how to use a combination of specific techniques to ensure flexibility, enforcement, and isolation of non-conforming clients.

31. The '786 patent is not directed to an abstract idea because it claims a specific technique to secure a computer network. The claims explain how they accomplish that goal. The claims check for conformance with security policies by examining a token, but then explain what to do next if the check fails. In particular, the claims isolate non-conforming clients to a subset of VLANs, logically separated from the rest of the network, and from which the clients can safely update their security policies. And the claims ensure that such clients are restricted to the subnet until they conform using an extensible authentication protocol.

32. The claimed invention overcame the drawbacks of prior art security systems. Unlike the prior art, the claimed invention is not client-dependent, ensuring network security by using active format security policies that can be obtained from a network server or webpage and automatically update the client, and as such can more easily react to new threats. In addition, on a network-wide level, the claimed invention checks for conformance, and securely ensures that non-conforming clients are safely isolated using an EAP that compliments the system's server focused model. The combination of these steps yields a specific and concrete improvement to secured

computer networks to overcome problems specifically arising in the realm of computer networks, and in a manner that could only be implemented in that environment.

33. The use of an extensible authentication protocol (EAP) and restricting non-conforming clients to a subset of virtual local area networks using the EAP in the manner claims was not conventional at the time of the application. Both of which were expressly added through claim amendments to overcome the prior art during prosecution. Ex. 7 at 11; Ex. 8 at 2.

34. The prosecution history expressly emphasized that the prior art did not disclose "restricting client access to said network of a plurality of virtual local area networks (VLANs), by using an extensible authentication protocol (EAP) to authenticate the client as a valid user of only a subset of available virtual local area networks (VLANs) within the network .... " Ex. 7 at 11 (emphasis original). The patent office recognized that specific use of an EAP as nonconventional and at least one reason for issuing the claims.

35. On information and belief, Defendant makes, uses, offers for sale, sells, and/or imports certain products ("Accused Products"), such as the F5 Networks BIG-IP Access Policy Manager (APM), that directly infringe, literally and/or under the doctrine of equivalents, claims 1–18 of the '786 Patent.

36. Defendant also knowingly and intentionally induces infringement of claims 1–18 of the '786 Patent in violation of 35 U.S.C. § 271(b). At least through the filing and service of this Complaint, Defendant has knowledge of the '786 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '786 Patent, Defendant continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website) to use the Accused Products in ways that directly infringe the '786 Patent. Defendant does so knowing and intending that its customers and end users will commit these infringing acts. Defendant also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '786 Patent, thereby specifically intending for and

inducing its customers to infringe the '786 Patent through the customers' normal and customary use of the Accused Products.

37. The Accused Products satisfy all claim limitations of claims 1–18 of the '786 Patent. A claim chart comparing independent claim 1 of the '786 Patent to the representative Accused Product, F5 Networks BIG-IP Access Policy Manager (APM), is attached as Exhibit 9.

38. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Defendant has injured Plaintiff and is liable for infringement of the '786 Patent pursuant to 35 U.S.C. § 271.

39. As a result of Defendant's infringement of the '786 Patent, Plaintiff is entitled to monetary damages in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendant, together with interest and costs as fixed by the Court.

40. Defendant's infringing activities have injured and will continue to injure Plaintiff unless and until this Court enters an injunction prohibiting further infringement of the '786 Patent, and, specifically, enjoining further manufacture, use, sale, importation, and/or offers for sale that come within the scope of the patent claims.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that Defendant has infringed, either literally and/or under the doctrine of equivalents, the'507 Patent and the '786 Patent;

b. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendant' infringement of the'507 Patent and the '786 Patent;

c. A judgment and order requiring Defendant to provide an accounting and to pay supplemental damages to Plaintiff, including without limitation, pre-judgment and post-judgment

interest;

d. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant; and

e. Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: August 11, 2020

Respectfully submitted,

/s/ Reza Mirzaie

Reza Mirzaie (CA SBN 246953)
rmirzaie@raklaw.com
Marc A. Fenster (CA SBN 181067)
Email: mfenster@raklaw.com
Brian D. Ledahl (CA SBN 186579)
Email: bledahl@raklaw.com
Benjamin T. Wang (CA SBN 228712)
Email: bwang@raklaw.com
Paul A. Kroeger (CA SBN 229074)
Email: pkroeger@raklaw.com
Kent N. Shum (CA SBN 259189)
kshum@raklaw.com
Jonathan Ma (CA SBN 312773)
jma@raklaw.com
RUSS AUGUST & KABAT
12424 Wilshire Blvd. 12th Floor
Los Angeles, CA 90025
Phone: (310) 826-7474

Attorneys for Plaintiff Proven Networks, LLC